9. นโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัท (Privacy Policy)

บริษัทเอสซีจี เซรามิกส์ จำกัด (มหาชน) ("บริษัท") เคารพสิทธิความเป็นส่วนตัวของลูกค้า ผู้ถือหุ้น พนักงานของบริษัท และบุคคลต่าง ๆ ที่เกี่ยวข้องกับบริษัท และเพื่อให้เกิดความมั่นใจว่าบุคคลดังกล่าวจะได้รับความคุ้มครองสิทธิอย่างครบถ้วนตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล คณะกรรมการบริษัทเอสซีจี เซรามิกส์ จำกัด (มหาชน) จึงอนุมัติให้ใช้นโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัท (Privacy Policy) เพื่อให้บริษัทมีหลักเกณฑ์ กลไก มาตรการกำกับดูแล และการบริหารจัดการข้อมูลส่วนบุคคลอย่างชัดเจนและเหมาะสม

1. <u>ขอบเขตการบังคับใช้</u>

นโยบายการคุ้มครองข้อมูลส่วนบุคคลนี้ ใช้บังคับกับบริษัท พนักงานของบริษัท และบุคคลที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของบริษัท

2. <u>คำนิยาม</u>

2.1. การประมวลผล (Processing) หมายถึง การดำเนินการใด ๆ กับข้อมูลส่วนบุคคล เช่น การเก็บ รวบรวม บันทึก จัดระบบ ทำโครงสร้าง เก็บรักษา ปรับปรุง เปลี่ยนแปลง กู้คืน ใช้ เปิดเผย ส่งต่อ เผยแพร่ โอน ผสมเข้าด้วยกัน ลบ ทำลาย

2.2. ข้อมูลส่วนบุคคล (Personal Data) หมายถึง ข้อมูลที่เกี่ยวกับบุคคลธรรมดา ซึ่งทำให้สามารถระบุตัวตนของบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ นามสกุล อีเมล เบอร์โทรศัพท์ IP Address รูปภาพ เชื้อชาติ ศาสนา ความคิดเห็นทางการเมือง ข้อมูลทางพันธุกรรม ข้อมูลทางชีวภาพ (Biometric Data)

2.3. เจ้าของข้อมูลส่วนบุคคล (Data Subject) หมายถึง บุคคลธรรมดาที่ข้อมูลส่วนบุคคลสามารถระบุตัวตนของบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม

2.4. ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) หมายถึง บุคคลธรรมดาหรือนิติบุคคล ซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล

2.5. ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) หมายถึง บุคคลธรรมดาหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

2.6. บริษัท หมายถึง บริษัทเอสซีจี เซรามิกส์ จำกัด (มหาชน) และบริษัทย่อยตามงบการเงินรวมของบริษัทเอสซีจี เซรามิกส์ จำกัด (มหาชน)

3. <u>นโยบายการคุ้มครองข้อมูลส่วนบุคคล: ด้านการกำกับดูแลการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Governance)</u>

3.1. บริษัทจะจัดให้มีโครงสร้างการกำกับดูแลข้อมูลส่วนบุคคล เพื่อกำหนดวิธีการและมาตรการที่เหมาะสมในการปฏิบัติตามกฎหมาย ดังนี้

(1) กำหนดให้มีโครงสร้างองค์กร (Organizational Structure) รวมทั้งกำหนดบทบาท ภารกิจ และความรับผิดชอบของหน่วยงานและผู้ปฏิบัติงานที่เกี่ยวข้องให้ชัดเจน เพื่อสร้างกลไกการกำกับดูแล การควบคุม ความรับผิดชอบ การปฏิบัติงาน การบังคับใช้ และการติดตามมาตรการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมาย และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัท

(2) แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท (Data Protection Officer: DPO) โดยมีบทบาทและหน้าที่ตามที่กำหนดในนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัท

3.2. บริษัทจะจัดทำนโยบาย (Policy) มาตรฐานการปฏิบัติงาน (Standards) แนวปฏิบัติ (Guidelines) ขั้นตอนปฏิบัติ (Procedures) และเอกสารอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมาย และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัท

3.3. บริษัทจะจัดให้มีกระบวนการบริหารการปฏิบัติตามนโยบาย (Policy Management Process) เพื่อควบคุมดูแลให้มีการปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัทอย่างต่อเนื่อง

3.4. บริษัทจะดำเนินการฝึกอบรมพนักงานของบริษัทอย่างสม่ำเสมอ เพื่อให้พนักงานของบริษัทตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคล และทำให้มั่นใจได้ว่าพนักงานของบริษัทที่เกี่ยวข้องทุกคนผ่านการฝึกอบรม และมีความรู้

ความเข้าใจในการคุ้มครองข้อมูลส่วนบุคคล และปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัท

4. **นโยบายการคุ้มครองข้อมูลส่วนบุคคล: ด้านการประมวลผลข้อมูลส่วนบุคคล (Personal Data Processing)**

4.1. บริษัทจะประมวลผลข้อมูลส่วนบุคคลทั้งในฐานะผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคลให้ถูกต้องตามกฎหมาย เป็นธรรม โปร่งใส และคำนึงถึงความถูกต้องของข้อมูลส่วนบุคคล ทั้งนี้ การกำหนดขอบเขตวัตถุประสงค์การประมวลผลข้อมูลส่วนบุคคล และระยะเวลาในการจัดเก็บข้อมูลส่วนบุคคล ให้ทำได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายและแนวทางการดำเนินธุรกิจของบริษัท อีกทั้งบริษัทจะดำเนินการรักษาความลับ ความถูกต้องสมบูรณ์ และความปลอดภัยของข้อมูลส่วนบุคคลอย่างเพียงพอ

4.2. บริษัทจะจัดให้มีกระบวนการและการควบคุมเพื่อบริหารจัดการข้อมูลส่วนบุคคลในทุกขั้นตอนให้สอดคล้องกับกฎหมาย และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัท

4.3. บริษัทจะจัดทำและรักษาบันทึกการประมวลผลข้อมูลส่วนบุคคล (Records of Processing: RoP) สำหรับบันทึกรายการและกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล ให้สอดคล้องกับกฎหมาย รวมทั้งจะปรับปรุงบันทึกการประมวลผลข้อมูลส่วนบุคคลเมื่อมีการเปลี่ยนแปลงรายการหรือกิจกรรมที่เกี่ยวข้อง

4.4. บริษัทจะจัดให้มีกระบวนการที่ชัดเจนเพื่อให้มั่นใจได้ว่าการแจ้งวัตถุประสงค์การเก็บรวบรวมและรายละเอียดการประมวลผลข้อมูลส่วนบุคคล (Privacy Notices) และการขอความยินยอม จากเจ้าของข้อมูลส่วนบุคคลสอดคล้องกับกฎหมาย รวมทั้งจัดให้มีมาตรการดูแลและตรวจสอบในเรื่องดังกล่าว

4.5. บริษัทจะจัดให้มีกลไกการตรวจสอบความถูกต้องของข้อมูลส่วนบุคคล รวมทั้งจัดให้มีกลไกการแก้ไขข้อมูลส่วนบุคคลให้ถูกต้อง

4.6. ในกรณีที่บริษัทส่ง โอน หรือให้บุคคลอื่นใช้ข้อมูลส่วนบุคคล บริษัทจะจัดทำข้อตกลงกับผู้ที่รับหรือใช้ข้อมูลส่วนบุคคลนั้นเพื่อกำหนดสิทธิและหน้าที่ให้สอดคล้องกับกฎหมาย และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัท

4.7. ในกรณีที่บริษัทส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ บริษัทจะปฏิบัติให้สอดคล้องกับกฎหมาย

4.8. บริษัทจะทำลายข้อมูลส่วนบุคคลเมื่อครบกำหนดระยะเวลา โดยปฏิบัติให้สอดคล้องกับกฎหมายและแนวทางการดำเนินธุรกิจของบริษัท

4.9. บริษัทจะประเมินความเสี่ยงและจัดทำมาตรการเพื่อบรรเทาความเสี่ยง และลดผลกระทบที่จะเกิดขึ้นกับการประมวลผลข้อมูลส่วนบุคคล

5. **นโยบายการคุ้มครองข้อมูลส่วนบุคคล: ด้านการรองรับการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights)**

บริษัทจะจัดให้มีมาตรการ ช่องทาง และวิธีการเพื่อให้เจ้าของข้อมูลส่วนบุคคลใช้สิทธิของตนได้ตามที่กฎหมายกำหนด รวมทั้งจะดำเนินการบันทึก และประเมินผลการตอบสนองต่อคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

6. **นโยบายการคุ้มครองข้อมูลส่วนบุคคล: ด้านการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (Personal Data Security)**

6.1. บริษัทจะจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลอย่างเพียงพอ รวมทั้งดำเนินการป้องกันไม่ให้เกิดการรั่วไหลของข้อมูลส่วนบุคคลและการนำข้อมูลส่วนบุคคลไปใช้โดยไม่ได้รับอนุญาต

6.2. บริษัทจะจัดให้มีนโยบายการบริหารจัดการเหตุการณ์ผิดปกติที่เกี่ยวข้องกับข้อมูลส่วนบุคคล (Privacy Incident Management Policy) และแนวทางการตอบสนองต่อเหตุการณ์ผิดปกติ (Incident Response Program) เพื่อให้สามารถระบุและจัดการกับเหตุการณ์ผิดปกติที่เกี่ยวข้องกับข้อมูลส่วนบุคคลได้อย่างทันท่วงที

6.3. บริษัทจะจัดให้มีกระบวนการแจ้งเจ้าของข้อมูลส่วนบุคคล รวมถึงเจ้าพนักงานของรัฐ ผู้ควบคุมข้อมูลส่วนบุคคล (ในกรณีที่บริษัทเป็นผู้ประมวลผลข้อมูลส่วนบุคคล หรือเป็นผู้ควบคุมข้อมูลส่วนบุคคล

ร่วมกัน) และบุคคลอื่น ให้สอดคล้องกับกฎหมาย

7. <u>นโยบายการคุ้มครองข้อมูลส่วนบุคคล: ด้านการกำกับให้เกิดการปฏิบัติตามมาตรการคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Compliance)</u>

7.1. บริษัทจะจัดให้มีกระบวนการติดตามในกรณีที่กฎหมายเปลี่ยนแปลงไป และปรับปรุงมาตรการคุ้มครองข้อมูลส่วนบุคคลให้ทันสมัยและสอดคล้องกับกฎหมายอยู่เสมอ

7.2. บริษัทจะจัดให้มีการทบทวนและปรับปรุงนโยบาย (Policy) มาตรฐานการปฏิบัติงาน (Standards) แนวปฏิบัติ (Guidelines) ขั้นตอนปฏิบัติ (Procedures) และเอกสารอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลเป็นประจำ เพื่อให้ทันสมัยสอดคล้องกับกฎหมายและสถานการณ์ในแต่ละช่วงเวลา

8. <u>บทบาท หน้าที่ และความรับผิดชอบ</u>

8.1. คณะกรรมการบริษัท มีบทบาท หน้าที่ และความรับผิดชอบดังต่อไปนี้

(1) กำกับให้เกิดโครงสร้างการกำกับดูแลข้อมูลส่วนบุคคล และการควบคุมภายในที่เกี่ยวข้องของบริษัท เพื่อให้เกิดการปฏิบัติตามกฎหมาย และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัท

(2) กำกับดูแลและสนับสนุนให้บริษัทดำเนินการคุ้มครองข้อมูลส่วนบุคคลให้มีประสิทธิภาพ และสอดคล้องกับกฎหมาย

8.2. คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (Privacy Committee)

ให้คณะจัดการบริหารความเสี่ยงของบริษัท (Risk Management Committee) ทำหน้าที่เป็นคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โดยมีบทบาท หน้าที่ และความรับผิดชอบดังต่อไปนี้

(1) จัดให้มีโครงสร้างการกำกับดูแลข้อมูลส่วนบุคคลและการควบคุมภายในที่เกี่ยวข้อง รวมถึงนโยบายการบริหารจัดการเหตุการณ์ผิดปกติที่เกี่ยวข้องกับข้อมูลส่วนบุคคล (Privacy Incident Management Policy) และแนวทางการตอบสนองต่อเหตุการณ์ผิดปกติ (Incident Response Program) เพื่อให้สามารถระบุและจัดการกับเหตุการณ์ผิดปกติที่เกี่ยวข้องกับข้อมูลส่วนบุคคลได้อย่างทันท่วงที

(2) ประเมินประสิทธิภาพการปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัท และรายงานผลการประเมินดังกล่าวให้คณะกรรมการบริษัททราบเป็นประจำอย่างน้อย 1 ครั้งต่อปี รวมถึงควบคุมดูแลให้มั่นใจได้ว่าความเสี่ยงต่าง ๆ ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลได้รับการจัดการและมีแนวทางการบริหารความเสี่ยงที่เหมาะสม

(3) กำหนดและทบทวนมาตรฐานการปฏิบัติงาน (Standards) และแนวปฏิบัติ (Guidelines) เพื่อให้การดำเนินงานของบริษัท สอดคล้องกับกฎหมาย และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัท

(4) แต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท (DPO)

8.3. ผู้บริหาร มีบทบาท หน้าที่ และความรับผิดชอบในการติดตามควบคุมให้หน่วยงานที่ดูแลปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัท และส่งเสริมการสร้างความตระหนักรู้ให้เกิดขึ้นกับพนักงานของบริษัท

8.4. เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท (DPO) มีบทบาท หน้าที่ และความรับผิดชอบตามที่กฎหมายกำหนด ซึ่งรวมถึงหน้าที่ดังต่อไปนี้

(1) รายงานสถานะการคุ้มครองข้อมูลส่วนบุคคลให้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบอย่างสม่ำเสมอ และจัดทำข้อเสนอแนะเพื่อปรับปรุงการคุ้มครองข้อมูลส่วนบุคคลของบริษัทให้ทันสมัยและสอดคล้องกับกฎหมายอยู่เสมอ

(2) ให้คำแนะนำพนักงานของบริษัท เกี่ยวกับการปฏิบัติตามกฎหมาย และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัท

(3) ตรวจสอบการดำเนินงานของหน่วยงานในบริษัท ให้เป็นไปตามกฎหมาย และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัท

8.5. พนักงานของบริษัท มีบทบาท หน้าที่ และความรับผิดชอบดังต่อไปนี้

(1) ปฏิบัติให้สอดคล้องกับนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัท มาตรฐานการปฏิบัติงาน (Standards) แนวปฏิบัติ (Guidelines) ขั้นตอนปฏิบัติ

(Procedures) และเอกสารอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(2) รายงานเหตุการณ์ผิดปกติที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล และการไม่ปฏิบัติตามกฎหมาย และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัทให้ผู้บังคับบัญชาทราบ

9. **<u>โทษของการไม่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัท</u>**

การไม่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัท อาจมีความผิดและถูกลงโทษทางวินัย รวมทั้งอาจได้รับโทษตามที่กฎหมายกำหนด